

REMARKS

In the present Office Action, the Examiner has rejected claims on various grounds under 35 U.S.C. §§ 101, 112 and 103. Applicants request that the Examiner reconsider the application in view of the amendments and remarks contained herein.

I. Specification Objections

In accordance with the Examiner's suggestion, the Abstract has been amended to correct the noted typographical error.

II. Claim Objections

In the Office Action, the Examiner has objected to claim 4 based on its similarity to claim 3. Applicant has submitted herewith an amended claim 4 to correct the inadvertent duplication.

III. Claim Rejections under 35 U.S.C. § 101

While the Applicants disagree with the Examiner's assertion regarding § 101 particularly in view of the recent decision in *Ex Parte Lundgren*, 76 USPQ2d 1385 (BdPatApp&Int 2005), Applicant has nevertheless withdrawn claims 17-20 and 38 solely for purposes of expediting the patenting process.

IV. Claim Rejections under 35 U.S.C. § 112

The Examiner has rejected claims 1-11 under 35 U.S.C. § 112, citing various antecedent basis issues. Applicants have amended these claims to address the issues cited by the Examiner. Accordingly, Applicants request that the rejections be withdrawn.

Moreover, as requested by the Examiner, Applicants have also reviewed the claims of the application to address any other such formality or readability issues that are evidently an inadvertent result of the translation process. In so doing, Applicants have made additional corrections to the claims as shown in the amendment simply for purposes of addressing such

issues and without intending to change the scope of the original claims.

V. Claim Rejections under 35 U.S.C. § 103

A. Rejections based on Lotspiech

The Examiner has rejected claims 1-6, 12-13, 21, 23-27, 35 and 37 as being obvious over Lotspiech (U.S. Patent no. 6,609,116) ("*Lotspiech*") in view of Caronni et al (U.S. 6,049,878) ("*Caronni*"). Similarly, claims 14, 22 and 36 stand rejected over the above combination of references in further view of Ishiguro (U.S. Patent no. 5, 796,839) ("*Ishiguro*"). Thus, the Examiner's rejection of claims 1-6, 12-14, 21-27 and 35 to 37 is based in part on the disclosure of *Lotspiech*. For the following reasons, Applicant requests that the Examiner withdraw the rejections. Applicant's invention is not obvious over the cited art.

Significantly, claim 1 refers to the following invention:

1. An information recording device for recording the information on a recording medium, comprising:

...

encryption means...

said encryption means detecting, in encrypting and storing content for said recording medium, the latest usable key renewal block from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself; said encryption means encrypting the data to be stored on said recording medium using the encrypting key obtained on decrypting the detected latest usable key renewal block.

In support of the rejection, the Examiner suggests that such an element is present at col. 4, lines 16-20 and col. 5, line 3 to col. 6, line 64) of the *Lotspiech* reference. Applicants disagree. For example, in the cited portions of the relied on reference, *Lotspiech* states:

When a user wants a player/recorder to record content onto a blank medium 16, the logic of FIG. 8 can be invoked by the associated encryption module 22. It is to be understood that each content is broadcast with the latest CMKC. Accordingly, at block 60 the player/recorder 14 compares the level of the new media key block with the level of the old media key block on the blank media sought to be used. When the old media key block is at least as current as the new (broadcast content) media key block, the player/recorder simply decrypts an "old" media key "k<sub>1</sub>", which is common to both the content and the blank medium, and then uses the old media key to encrypt the content and record it on the blank medium 16.

On the other hand, when compromised player/recorders have been suspected between the time the medium 16 was produced and the content was produced (and, hence, when the level of the content is higher, i.e., more recent than the level of the medium 16), the logic moves from block 60 to block 62. At block 62, the medium's CMKC is read, and the player/recorder 14 uses the appropriate device key to decrypt the old media key "k<sub>1</sub>" from the medium at block 64.

*Lotspiech*, col. 6, lines 35-52. It is clear from this disclosure that the system of *Lotspiech* is not a key renewal system based on detecting the latest of the usable key renewal blocks from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself. Rather, the system of *Lotspiech* simply detects an old media key block of the medium and decrypts an old media key for encrypting and storing content.

Thus, the relied on aspects of the system of *Lotspiech* described therein are much different from Applicants' invention. In view of the cited disclosure, *Lotspiech* should be viewed as teaching away from the Applicants' invention. Accordingly, the Examiner has not set forth a *prima facie* claim of obviousness for independent claim 1 since a feature of Applicants' invention

is not disclosed or taught in the relied on sections of *Lotspiech*.

Similarly, to the extent that the Examiner sets forth a comparable rejection of independent claims 12, 21 and 35 based on *Lotspiech*, these claims may be compared to the subject matter of claim 1. In short, the Examiner's reliance on *Lotspiech* is insufficient to establish a *prima facie* case of obviousness for independent claims 12, 21 and 35. For example, in its scheme of recording data to a recording medium, claim 12 defines, *inter alia*,

a step of detecting a latest usable one of key renewal blocks stored in the recording medium and the key renewal block stored in said memory means of the information recording device itself;

a step of decrypting the detected latest usable key renewal block, at said detection step, using at least the node key or the leaf key held in said information recording device, to calculate the encrypting key used in encrypting data stored in said recording medium; and

a step of encrypting recording data for said recording medium, using the calculated encrypting key, to store the encrypted data on the recording medium.

As previously discussed with regard to the provisions relied on in the disclosure of *Lotspiech*, the elements of claim 12 are not present in the cited art.

Similarly, claim 21 defines, *inter alia*,

renewing means for comparing, in accessing the recording medium, a version of a key renewal block stored in the recording medium to that of the key renewal block owned by the information recording device itself, and for writing a key renewal block of a new version on the recording medium if the key renewal block of the new version is the key renewal block stored in the memory means of the recording device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

Again, the relied on provisions of *Lotspiech* in view of the prior discussion do not teach or suggest the invention of claim 21.

Lastly, claim 35 at least recites the following:

a detection step of detecting a latest usable one of key renewal blocks stored on the recording medium and a key renewal block stored in a memory means of the recording or reproducing device; and

At least this element of claim 35 is not present in the relied on provisions of *Lotspiech* as previously discussed.

Accordingly, Applicants request that the Examiner withdraw the rejections of claims 1-6, 12-14, 21-27 and 35 to 37. Applicants respectfully submit that the claims are in condition for allowance. Furthermore, while Applicants disagree with other aspects of the Examiner's rejection, Applicants submit that in view of the absence of at least the discussed elements in the cited reference any further discussion is unnecessary at this time.

B. Rejections based on *Ishiguro*

Claims 7-11, 15-16 stand rejected as being obvious over *Ishiguro* in view of *Caronni*. The Examiner has also rejected claims 28-34 as being obvious over *Ishiguro* in view of *Caronni* and *Lotspiech*. For at least the following reasons, Applicants request that the Examiner withdraw the rejection.

Amended claim 7 defines:

An information reproducing device for reproducing the information from a recording medium, comprising:

... encryption means for decrypting the key renewal block ...;

said encryption means detecting, in processing of decrypting the cipher data stored in said recording medium, the latest one of the key renewal block stored in the recording medium and the key renewal block stored in the memory means of the reproducing device itself, which has a version coincident with the

version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key renewal block.

Applicants' invention is not disclosed in the cited art. To this end, the Examiner has cited various sections of *Ishiguro* in reference to the above cited element. However, the relied on sections do not disclose an encryption means detecting the latest one of the key renewal block stored in the recording medium and the key renewal block stored in the memory means of the reproducing device itself, nor has the Examiner provided a specific cite comparable thereto.

Moreover, as previously discussed with regard to claim 1, the aspects of the Applicants' invention are not disclosed in *Lotspiech*. Thus, Applicants submit that independent claim 7 and its dependent claims 8-11 are in condition for allowance.

Similarly, the subject matter of independent claim 15 is not disclosed or rendered obvious over the disclosure of *Ishiguro*. To this end, independent claim 15 defines:

An information reproducing method in an information recording device adapted for recording the information for a recording medium, each of a plurality of such devices holding a node key unique to each node of a hierarchical tree structure having the plural respective information recording devices operating as leaves, and a leaf key unique to each information recording device, said method comprising:

...  
a step of detecting a latest one of a key renewal block stored in the recording medium and a key renewal block stored in a memory means of the recording device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced;

As previously discussed with regard to *Ishiguro*, Applicants submit that the claimed invention is not disclosed in the cited

art. Accordingly, Applicants submit that independent claim 15 and dependent claim 16 are in condition for allowance.

Finally, independent claim 28 may be compared with the subject matter of claim 7. For example, claim 28 claims:

An information reproducing device for reproducing the information from a recording medium, each information reproducing device comprising:

renewal means for comparing, in accessing the recording medium, a version of a key renewal block stored in the recording medium to that of the key renewal block owned by the reproducing device itself, and for writing the key renewal block of a new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of the reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

As previously discussed, *Ishiguro* does not disclose such an invention. In the present Office Action, the Examiner appears to recognize this conclusion in that the Examiner has cited only *Lotspiech* for the recited aspect of the Applicants' invention. Office Action at 10. However, as previously discussed, *Lotspiech* actually teaches away from this aspect of the Applicants' invention in that *Lotspiech* simply teaches the use of old media keys for encrypting rather than Applicants' claimed comparison and writing of key renewal blocks. For at least this reason, Applicant respectfully submits that the Examiner has not set forth a *prima facie* claim of obviousness with regard to claims 28-35. Thus, Applicants request that independent claim 28 and dependent claims 29-35 be allowed and the rejection withdrawn.

While Applicants disagree with other aspects of the Examiner's rejection of the claims based on *Ishiguro* and its combination with other references, Applicants submit that in view of the absence of at least the discussed elements in the

art cites relied on, any further discussion is unnecessary at this time.

VI. Conclusion

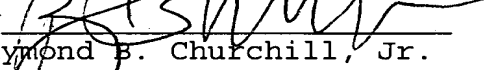
As it is believed that all of the rejections set forth in the Official Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he/she telephone applicant's attorney at (908) 654-5000 in order to overcome any additional objections which he might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: April 18, 2006

Respectfully submitted,

By   
Raymond B. Churchill, Jr.  
Registration No.: 44,617  
LERNER, DAVID, LITTENBERG,  
KRUMHOLZ & MENTLIK, LLP  
600 South Avenue West  
Westfield, New Jersey 07090  
(908) 654-5000  
Attorney for Applicant